International Journal of Computer Networking,
Wireless and Mobile Communications (IJCNWMC)
ISSN(P): 2250-1568; ISSN(E): 2278-9448
Vol. 4, Issue 4, Aug 2014, 27-32

TRANS STELLAR
• Journal Publications • Research Consultancy

TRUSTED ENERGY EFFICIENT CLUSTER BASED ROUTING IN MANET

JASPINDER SINGH & MEENAKSHI SHARMA

Department of Computer Science & Engineering, SSCET, Badhani, Pathankot, Punjab, India

ABSTRACT

Mobile Ad-hoc will be a vital part of next generation network due to its flexibility, infrastructure less nature, and ease to maintenance, auto configuration, self-administration capabilities, and cost effectiveness. In this paper propose an algorithm technique – which is "trusted Signal and Energy Efficient Clustering (TSEEC)" base on the Secure routing and minimized the flooding strategies. It is emphasis that cluster maintenance and formation at low cost the resources used that are signal strength, battery power and trusted value of the node. In this paper signal strength and trusted value of node are distributed on network backbone using passive cache mechanism to reduce the flooding for route discovery hence reduce the routing overhead and efficient use of resources

KEYWORDS: Trust Value, Cluster Head, Energy Strength, Signal Strength, Routing, CBRP, and MANET

INTRODUCTION

Mobile Ad-hoc Network is a wireless network of mobile computing devices that are connected by multi-hop wireless links. MANET are highly dynamic network as there is deployment of central base station is neither economic nor easy. The node involved in MANET function as router as well as host to exchange packets to other nodes in the network. In MANET node has properties to move and synchronize with their neighbour's. Due to mobility of nodes, connection in the network can change dynamically and node can add and remove dat any time. MANET has no fixed fundamental Structure. MANET could potentially be used in various applications such as mobile classrooms, battlefield communication, remote conferencing and disaster relief applications.

MANET classified by two categories on the basis of their routing techniques in clusters. These techniques are flat routing and cluster base routing. In flat routing all nodes transfer a data to base station for communication [2]. In cluster base routing has cluster head, which responsible for route between node and base stations. Cluster base routing is superior then flat routing in energy efficiency, due to decreasing amount of data transmission.

- **Lexis used in CBRP**
  - **Node ID:** Unique Identification of all node within a cluster e.g. IP Address and MAC address of the nodes.
  - **Cluster:** A collection of nodes in which a particular node elected as head node. Each cluster has unique ID of the cluster head. Cluster may be overlapping or disjoint group of nodes. Nodes belong to the cluster has recognized by their head ID.
  - **Cluster Members:** Nodes which are not participate in neither cluster gateway nor a cluster head are represented with the members of the cluster.
  - **Cluster Head:** Leader node of the cluster which play vital role for routing and data transferring.

- **Cluster Gateways:** Node that link information between two clusters.

- **Theoretical Data Arrangements Used in CBRP [2]**

  It has following fields:

  - Identificationof Linked cluster head
  - Gateways of the adjoining clusters.
  - The role of the neighbours.

ADJOINING_CLUSTER_ID	GATEWAY	LINK_ STATUS

Figure 1: Format of Cluster Adjoining Table

- **Neighbour Table [2]**

  It has following fields

  - The ID of the neighbor that it has connectivity with
  - Role of the neighbor.
  - Link status.

NEIGHBOR_ID	LINK-STATUS	ROLE

Figure 2: Format of Neighbour Table

But there are several problem faced by the CBRP which are energy consumed by the head node, security, privacy and energy consumed by the hidden nodes. Due to these problems cluster has short life time. In this paper, we propose an algorithm technique – whichis “trusted energy effective cluster base routing” base on the secure routing and minimized the flooding strategies. It is emphasis that cluster maintenance and formation at low cost the resources that used are signal strength, battery power and trusted value of the node. In this paper trusted value of node are distributed on backbone using passive cache mechanism to reduce the flooding for route discovery hence reduce the routing overhead and efficient use of resources. The rest of this paper is organized as follows. Section 2 reviews some related work; Section 3 gives a proposed work; Section 4 gives an algorithm; we conclude with Section 5

RELATED WORK

In this section we wil lgive overview on different Routing Protocols in MANET. PritiGarg, et. al “Comparative Performance Analysis of Two Ad-hoc Routing Protocols”, International Conference on Network and Electronics Engineering IPCSIT vol.11, pp 99-104, 2011 [2]. The author of this paper reports various issues by analyse the comparative performance of Ad hoc routing protocols; Its associated on-demand and hybrid protocol;these protocols are TORA (temporally ordered routing algorithm) and DSR (Dynamic Source Routing). This paper compare these protocols under different environmental circumstances and calculates their comparative performance with respect to numerical metrics; throughput, average delay, packet delivery ratio and routing load under the simulation NS-2 for the complete simulation results. It has been found that DSR and TORA protocol and variation arises in mobility of packets, time intermission between the packets transmitted and packet size of packets transmitted in throughout.

Numerous mechanisms of cluster head choice occur with an objective to deliver established and effective routing in the MANET system [1], [4], and [5]. Various mechanisms support not altering the cluster head to ease the signalling overhead involved in the process, which also makes the chosen node usage of their resources higher.

PROPOSED METHODOLOGY

The main disadvantage that identified in related work is smaller lifetime of the cluster head. Cluster head dies because of extra power indulgence. The main focus of propose the TSEEC (trusted Signal and Energy Efficient Clustering) algorithm is preventing the cluster head and re-selected the cluster head when energy and signal fall to the threshold value and calculate the trust value between the nodes according to their interaction behaviours. Base on that trust value of node we judge that connection between the two node are trusted or not. According to signal strength, energy strength and trusted connection of the node cluster head is selected. Data structure to maintain the cluster head are follows:

- **Improved Data Format of Hello Message**

Node participant's MANET transmission hello message in hello _intervals of Seconds. Seconds; a nodes HELLO message containits 'Cluster Adjacency Table'. Figure 3 show the modified head format of the hello message new field added in hello messages are Signal Strength', 'Battery Power Level' & 'trust value of node', which help to formation of cluster head (CH).

Node ID	Node Status	Signal Strength	Battery Power Level	Trusted Value
……	……	……	……	……..
Neighbour ID	Neighbour Status	Connection Status	Adjacent Cluster ID	Link trusts
…….	……	……	……	…...

Figure 3: Layout of HELLO Packet

- **Proposed Data Structure for Head Table**

Cluster head maintain the signal strength, power level and trust value of all node and proposed a new format of cluster head. The behaviour of the node analysed by the trust value. If the node are untrusted then cluster head refuse and provide updating in backbone of passive cache and malicious node will shielded by cluster for ever.

Node ID	Signal Strength	Power Strength	Trusted value

Figure 4: Layout of Head Table

- **Calculation of Truth Value**

Trust value define the amount of trust between the trust-or and trustee node. The calculation of trust value can be done by using continuous real number -1 and +1. The negative number show the amount of distrust. -1 denotes the whole distrust the node. Positive number show the complete trust between the nodes. Trust value dynamically change due to the behaviour of the nodes. Trusted value iscalculated by trusted vector which contain the value of shared public and private keys. This keys exchanging shows the behaviour of the nodes. In key

Parameter	Value
Trusted vector	Key exchanging
Routing Table	No of packets sent by node from the beginning
Packet received	No of packets received by nodefrom the beginning

Figure 5: Trusted Data Structure Format

In key exchanging process malicious node often drop the packet because of not proper key exchanging and calculated by the equation.

$$TE(V) = \frac{\sum_{i=1}^{B} C_i \times V_i}{\sum_{i=1}^{B} C_i} \quad [\text{where} 1 \leq \text{TE(V)} \leq 0]$$

Where C_i is the Trust rating of node, $V_i$is the i^{th} bit of the trust value. Trust équation calculates the trust vector after the deliver the packets. And the un-trusted vector can be calculated by 1-TE(V).

- **Passive Cached Mechanism**

Passive cached mechanism reduce the flooding for route discovery. In this mechanism all route of trusted and untrusted nodes are requested and replies in the passive way. Information regarding the node is either trusted or nor are stored in network backbone. Network backbone is configuration of cluster head and gateways interconnect the entire network. Untrusted node once refuse by the cluster and provide updating in backbone of passive cache and malicious node will shielded by cluster for ever

CLUSTER FORMATION

After trusted the node each node in the network broadcast Hello message specified its ID, Signal Strength Current power level trusted value through the network backbone. Each node in the network compare their value of parameters like Signal Strength, energy etc. The node which has higher value of signal and power are declared as head node of the cluster. When the power and signal of cluster head that are most trusted node fall below the threshold value re-election of cluster head taken.

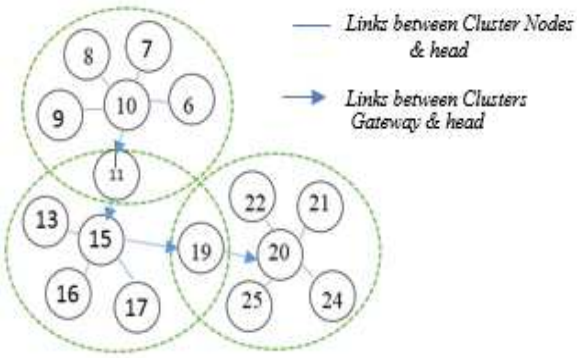

Figure 6: Cluster Formation

Figure 6' shows cluster architecture where 'node 10', 'node 15' and 'node 20' are cluster heads of clusters. 'Node11' and 'node 19' act as cluster gateways, and rest of them are cluster nodes or member nodes.

Node 10's Head Table

Node ID	Signal Strength (%)	Power Strength (%)
10	89	91
11	74	82
9	62	57
8	66	69
7	71	54
6	69	72

Node 20's Head Table

Node ID	Signal Strength (%)	Power Strength (%)
20	82	92
21	75	77
25	69	72
24	55	66
22	45	64
19	75	79

Node 15's Head Table

Node ID	Signal Strength (%)	Power Strength (%)
15	82	92
13	75	77
16	69	72
17	55	66
11	45	64
19	75	79

Node 15's Neighbor Hood

Neighbor Hood node ID	Neighbor Status	Link status or trust vlaue
19	member	T1
11	member	T1
13	member	T1
16	member	T1
17	member	T1

Node 6's Adjacent Table

Adjacent Cluster ID	Gateway	Link status or trust vlaue
15	11	T1

Node 16's Adjacent Table

Adjacent Cluster ID	Gateway	Link status or trust vlaue
10	11	T1
20	19	T1

Figure 7: Example of Table Maintained in Cluster Nodes

PROPOSED ALGORITHM

In this algorithm initially all node within the cluster is verified by sharing the keys between nodes. These sharing keys make all nodes trusted or untrusted according to behaviour of these nodes. After trusted the all nodes signal and energy of node if check and store all the information to the cache of the network backbone for future purpose and compare all power and signal of the nodes with the threshold value the select the cluster head. When the power and energy of the selected trusted cluster head falls below the threshold value the process of selection the cluster head will repeated.

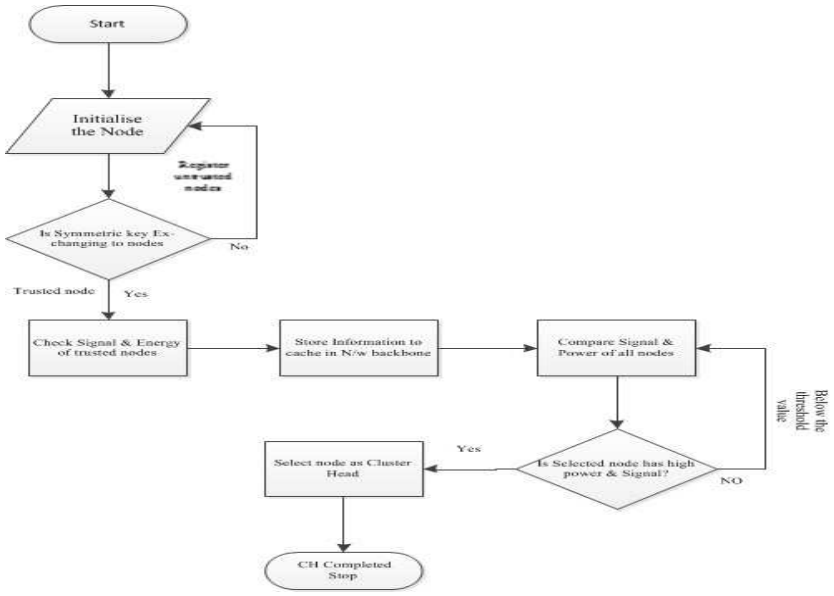

Figure 8: Flow Graph Representation of Algorithm

CONCLUSIONS

This paper represents a Trusted, signal and Energy Efficient Clustering (TSEEC). The main motive of this algorithmis to protect the node from malicious, hidden node and selfish node that used the resource of the other node in the clusters. The main motive of this paper is to keep alive the head node and avoid re-election of cluster head. Our future work is to simulate the proposed algorithm and also tried to find the more effective cryptographic techniques to protect the cluster head from the external attacker and hidden node.

REFERENCES

1. N. Chatterjee, A. Potluri and A. Negi, “A Self Organising Approach to MANET Clustering”, High Performance Computing, Oct. 13, 2006.
2. Alak Roy, ManasiHazarika and MrinalKantiDebbarma “Energy Efficient Cluster Based Routing in MANET” International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 2012
3. Utkarsh, Mukesh Mishra and SuchismitaChinara “ESAR: An Energy Saving Ad Hoc Routing Algorithm for MANET” IEEE- Fourth International Conferenceon Advanced Computing, ICo AC 2012.
4. J. Liu, Y. Lu, J. Xiao and F. Fu, “Secure Routing for Mobile Ad hoc Networks”, 8th ACIS International Conference, pp 314-318, 2007.
5. Yan Shuailing, Jiang Huawei, Wang Gaoping “An Improved Clustering Algorithm Based on MANET Network” IEEE International Symposium on IT in Medicine and Education, 2008.
6. C. R. Lin and M. Gerla. “Adaptive Clustering for mobile Wireless networks”.IEEE J. Select. Areas Common, Vol. 15, no.7, pp.1265-1275, Sep.1997.
7. Li Wang and Fei Gao “A Secure Clustering Scheme Protocol for MANET” International Conference on Multimedia Information Networking and Security, 2010.
8. K. Drira et al, ECGK “An efficient clustering scheme for group key management in MANETs”, Compute Commun (2010), doi:10.1016/j.com com.2010.
9. M. Carbone, M. Nielsen, and V. Sassone. “A formal model for trust in dynamic networks”, conf. on Software Engg and Formal Methods, 2003, pp 54-61.
10. Y. Wang and J. Vassileva, “Trust and Reputation Model in Peer-to-Peer Networks”, Proc. of IEEE Conference on P2P Computing, 2003, pp 150-160.
11. H. Deng, W. Li and D.P. Agrawal, “Routing Security in Wireless Ad hoc Networks”, University of Cincinnati, IEEE communication Magazine, 2002, pp.70-75.
12. M. S. Corson and A. Ephremides, “A Distributed Routing Algorithm for Mobile Wireless Networks”, ACM Journal, Wireless Networks, 1(1), 1995.